

purposes of authenticating user **25** and subscriber unit **30**, the processing within either base station **35** or one of the satellites is substantially the same. Base station **35** is typically a cellular or personal communications system (PCS) transceiver, but can be any other data communications node. The processing will be described with reference to a satellite. When user **25** requests access to communications system **10**, subscriber unit **30** transmits to satellite **15** using communications link **70**. Subscriber unit **30** is preferably a radio frequency (RF) transmitter. As will be described in more detail below, RF transmitters have unique signatures that can be used for identification. In addition to identification of subscriber unit **30**, it is desirable to authenticate user **25**. To that end, subscriber unit **30** measures biometric data from user **25** and transmits it to satellite **15**. "Biometric" as defined, for example, in U.S. Pat. No. 5,469,506 means a substantially stable physical characteristic of a person which can be automatically measured and characterized for comparison.

The use of biometric information for authentication of users has many advantages. A biometric "ID" can never be lost or stolen because the biometric information is a physical attribute of the holder. Additionally, with advances in technology, biometrics are quickly becoming the most reliable method of user authentication known.

HLR **55** includes a valid user profile for user **25** and subscriber unit **30**. The valid user profile includes a data-gram representing the RF signature of subscriber unit **30**, and biometric information for user **25** as measured by subscriber unit **30**. After receiving biometric information from user **25**, satellite **15** measures the RF signature of subscriber unit **30**. Satellite **15** then sends a message through satellite **20** to HGW **50** retrieving the valid user profile from HLR **55** (or from VLR **45**).

In a preferred embodiment, satellite **15** authenticates both user **25** and subscriber unit **30** by comparing biometric information and the RF signature of subscriber unit **30** to the valid user profile obtained from HLR **55**. Because both biometric information and RF signatures are subject to statistical variations, a perfect match is seldom made. Accordingly, satellite **15** determines a degree to which user **25** and subscriber unit **30** match a valid user profile, resulting in a probability that the request for access is authentic. The valid user profile also includes a threshold value, which the probability is compared against, to determine authenticity. The methods utilized may be any one of several, including contour distance measure, which is an average summation of differences of each of the parameters; a least mean square (LMS) error; weighted Gaussian density distribution matching; and any other weighted or non-weighted statistical measurement.

Multiple mobile users **25** can be valid users of subscriber unit **30**. HLR **55** includes valid user profiles for all valid registered users of subscriber unit **30** as measured by subscriber unit **30** for each user. Satellite **15**, when authenticating access, compares the biometric information and RF signature against all valid user profiles included in HLR **55**.

User **25** can also access communications system **10** through base station **35**. When a call request is made by user **25** through base station **35**, base station **35** receives the biometric information and the RF signature of subscriber unit **30**. Base station **35** receives a valid user profile from HLR **55** through either communications link **80** or PSTN **60**.

#### Subscriber Unit Authentication

RF transmitters have a unique spectral signature which can be used to distinguish one unit from another. The method

and apparatus of the present invention utilizes this unique signature to distinguish legitimate subscriber units from fraudulent subscriber units in communications system **10**. The technique of identifying transmitters using RF signatures is not new in the art, and has been previously used in military and intelligence applications. An example of an apparatus for characterizing a radio transmitter can be found in U.S. Pat. No. 5,005,210 issued Apr. 2, 1991, the contents of which are hereby incorporated by reference.

Despite good engineering design practices, all RF transmitters will transmit undesired signal components at frequencies within, and out of, a given bandwidth. These unwanted components originate in a variety of places in the transmission chain. For example, amplifier non-linearities, particularly in the output power amplifiers, produce harmonics and intermodulation distortion (IMD). Crystals used in oscillators in the RF unit also produce unique, non-zero sub-harmonics. Mixers further compound the production of undesired mixing and spurious responses. Since each transmitter is a unique combination of elements which produce a unique combination of these undesired spurs, harmonics, and IMDs, this information can be measured and used to identify and authenticate the particular RF transmitter.

Measurable RF characteristics unique to each transmitter go beyond the aforementioned spurious spectral content. Examples include, but are not limited to, turn on transmitting amplitude, frequency or phase modulation versus time, the time between turn on and onset of data, phase and frequency modulation during that delay, the initial amplitude, phase and frequency modulation when data transmission starts, transmission bit times, total times, timing jitter, rise and fall timing, carrier turn off time, modulation deviation and distortion, modulation phase, bit to bit modulation variations, demodulation spectrum, spurious transmitter data, etc. Some or all of these various characteristics can be used by communications system **10** for authentication of subscriber unit **30**.

#### User Authentication

The method and apparatus of the present invention uses biometric information describing user **25** to authenticate access. Biometric information used to authenticate access can consist of retinal eye scan data, iris eye scan data, fingerprint data, voice print data, palm pressure print data, facial thermography, or any other data that represents a unique feature of an individual user.

Biometric information used to authenticate access can include retinal eye scan data, which is a mapping of the retinal blood vessels of the human eye. Research suggests that no two human eyes share the same pattern of blood vessels. A retinal eye scan is typically performed by shining an infrared light through the pupil to the back of the eye. The results are recorded for comparison with known valid data previously collected from the authentic user. Because retinal eye scan data is unique to each user, this leads to very robust authentication methods.

The use of a retinal eye scanner is advantageous because a retinal eyescan of user **25** provides a highly reliable authentication through the use of unique characteristic of each user **25**. When retinal eyescan data is used, subscriber unit **30** includes a retinal eyescanner. When placing a call, user **25** places subscriber unit **30** such that a retinal eyescan is performed, and the retinal eyescan data is transmitted to satellite **15**. Biometric information can also include voice print data, such as vocoder coefficients generated by subscriber unit **30** when user **25** speaks a standard phrase into